REMARKS

By the present amendment, Claim 11 has been newly added. Claims 1-11 remain pending in the application, with Claims 1, 3, 6, 7, 10 and 11 being independent claims. Claims 1-10 are again rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by Akiyama (U.S. Patent Application Publication No. 2003/0002680 A1).

New independent Claim 11 recites, in part, a security deciphering method comprising: providing a hidden secret key (Kh) corresponding to intrinsic identification information; providing a cipher key (Ks); generating a personal secret key ({Ks}Kh) by the cipher key (Ks) by using the hidden secret key (Kh); and encoding/decoding data M using the hidden secret key (Kh), the cipher key (Ks); and the personal secret key ({Ks}Kh), thereby achieving improved security for transmitting/receiving the data M over public networks.

In the Advisory Action dated April 11, 2008 (the Advisory Action), the Examiner maintained his reliance on FIGS. 2, 3, 14, and paragraphs 107, 108, 188, 195 and 198 of Akiyama for anticipating all of the recitations of Claims 1-10, and stated that Applicant's arguments had been considered but were not persuasive.

The present invention relates to a security deciphering apparatus and method in which the data of a cipher key used to encipher data is obtained by decoding an enciphered version of the cipher key by using hidden identification (ID) information given to a terminal requesting the data.

In the previous Office Action dated December 19, 2008 (the Final Office Action), the Examiner merely copied Claims 1-10 and included areas in Akiyama where the Examiner believes these recitations are disclosed. In particular, the Examiner believes Akiyama anticipates the recitations in Claims 1-5 and 7-10 in FIGS. 2, 3, 14, and paragraphs 107 and 108, and believes that Akiyama anticipates the recitations of Claim 6 in paragraphs 188, 195 and 198.

Independent Claim 1 recites, in part, a security deciphering apparatus comprising: a hidden secret key storing unit for storing a hidden secret key (Kh) corresponding to intrinsic identification information; a first decoding unit for receiving via a public network a personal secret key ({Ks}Kh), generated by enciphering a cipher key (Ks) by using the hidden secret key (Kh), and decoding the personal secret key ({Ks}Kh) by using the hidden secret key (Kh), thereby obtaining the cipher key (Ks); and a second decoding unit for receiving via the public network enciphered data ({M}Ks), generated by enciphering data (M) by using the cipher key (Ks), and decoding the enciphered data ({M}Ks) by using the cipher key (Ks), thereby obtaining the data (M).

In the Final Office Action, the Examiner merely copied Claim 1 and identified FIG. 14, and paragraphs 107 and 108 of Akiyama as allegedly suggesting these recitations.

Paragraph 107 of Akiyama is shown below.

> "The broadcast station 200 broadcasts contents information ([Contents]Kch) which is encrypted using a channel key Kch prescribed for each channel, and appending information ([Appending]Km) which is containing a terminal ID, a channel key Kch, etc., and encrypted using a master key Km."

Paragraph 108 of Akiyama is shown below.

> "The appending information is used in giving a reception permission only to a user who has a broadcast reception contract and paid the reception fee. The reception device provided at each user's home receives the encrypted appending information ([Appending]Km) and decrypts it using the master key Km provided in that reception device. Then the terminal ID contained therein is compared with the terminal ID assigned to that reception device, and if they coincide, the channel key

Kch contained therein is stored into a database provided in that reception device and will be used in decrypting the encrypted contents information ([Contents]Kch)."

In these areas, Akiyama merely discusses the use of only two keys for encrypting and decrypting data in a broadcast station and a reception device, not three keys as in the present invention. The two keys described by Akiyama include a master key Km and a channel key Kch. The broadcast station encrypts and transmits data using the master key Km and the channel key Kch, and the reception device receives and decrypts data transmitted from the broadcast station using the master key Km and the channel key Kch. Encryption/decryption of data in Akiyama through the use of the master key Km and the channel key Kch operates differently from encoding/decoding data with the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) in the present invention.

Akiyama fails to teach the claimed invention because the claimed invention recites three keys including the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh). The hidden secret key (Kh) corresponds to intrinsic identification information. The cipher key (Ks) is used to generate the personal secret key ({Ks}Kh) by using the hidden secret key (Kh). These three keys, e.g. the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh), are recited in Claim 1 and are nowhere disclosed in Akiyama. Furthermore, Akiyama provides no disclosure that would motivate one skilled in the art at the time the invention was made to arrive at the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) recited in Claim 1.

Applicant respectfully submits that these areas of Akiyama fail to anticipate, and Akiyama provides no motivation whatsoever to modify the teachings thereof to provide the recitations of Claim 1.

Additional features of the invention recited in Claim 1 are found in dependent Claim 2. Dependent Claim 2 recites, in part, that the security deciphering apparatus of Claim 1 further

includes a personal secret key storing unit for storing the personal secret key ({Ks}Kh) received via the public network, and outputting the stored personal secret key ({Ks}Kh) to the first decoding unit under a control of the first decoding unit; and a cipher key storing unit for storing the cipher key (Ks) obtained by the first decoding unit, and outputting the stored cipher key (Ks) to the second decoding unit under a control of the second decoding unit.

In the Final Office Action, the Examiner merely copied Claim 2 and identified FIG. 14, and paragraph 108 of Akiyama as allegedly suggesting these recitations. Paragraph 108 of Akiyama is presented above with respect to Claim 1.

As discussed above, in these areas, Akiyama merely discusses the use of only two keys, e.g. the master key Km and the channel key Kch, for encrypting and decrypting data in a broadcast station and a reception device. Encryption/decryption of data in Akiyama through the use of the master key Km and the channel key Kch operates differently from encoding/decoding data with the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) in the present invention. Akiyama nowhere suggests the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) that are recited in Claim 2. Furthermore, Akiyama provides no disclosure that would motivate one skilled in the art at the time the invention was made to arrive at the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) recited in Claim 2.

Applicant respectfully submits that these areas of Akiyama fail to anticipate, and Akiyama provides no motivation whatsoever to modify the teachings thereof to provide the recitations of Claim 2.

Independent Claim 3 recites, in part, a data service providing apparatus for providing data requested by a communication terminal, the apparatus comprising: a data database for storing data (M) to be provided to the communication terminal; a hidden secret key database for storing a hidden secret key (Kh) corresponding to intrinsic identification information of a security deciphering module equipped in the communication terminal to decipher enciphered data; a

transmitting/receiving unit for performing communication with the communication terminal via a public network; a data enciphering unit for enciphering the data (M) by using a cipher key (Ks); a cipher key enciphering unit for enciphering the cipher key (Ks) by using the hidden secret key (Kh); and a control unit for controlling the enciphering operations of the data and cipher key enciphering units, and controlling the transmitting/receiving unit to provide the enciphered data ({M}Ks) and a personal secret key ({Ks}Kh) via the public network.

In the Final Office Action, the Examiner merely copied Claim 3 and identified FIG. 3, and paragraphs 107 and 108 of Akiyama as allegedly suggesting these recitations. Paragraphs 107 and 108 of Akiyama are presented above with respect to Claim 1.

As discussed above, in these areas, Akiyama merely discusses the use of only two keys, e.g. the master key Km and the channel key Kch, for encrypting and decrypting data in the broadcast station and the reception device. Encryption/decryption of data in Akiyama through the use of the master key Km and the channel key Kch operates differently from encoding/decoding data with the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) in the present invention. Akiyama nowhere suggests the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) that are recited in Claim 3. Furthermore, Akiyama provides no disclosure that would motivate one skilled in the art at the time the invention was made to arrive at the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) recited in Claim 3.

Applicant respectfully submits that these areas of Akiyama fail to anticipate, and Akiyama provides no motivation whatsoever to modify the teachings thereof to provide the recitations of Claim 3.

Additional features of the invention recited in Claim 3 are found in dependent Claim 4. Dependent Claim 4 recites, in part, that the data service providing apparatus of Claim 3 further includes a hidden secret key storing unit for storing the hidden secret key (Kh) corresponding to the intrinsic identification information of the security deciphering module; a first decoding unit

for decoding the personal secret key ({Ks}Kh) provided by the transmitting/receiving unit, by using the hidden secret key (Kh), thereby obtaining the cipher key (Ks); and a second decoding unit for decoding the enciphered data ({M}Ks) provided by the transmitting/receiving unit, by using the cipher key (Ks), thereby obtaining the data (M).

In the Final Office Action, the Examiner merely copied Claim 4 and identified FIGS. 3 and 14, and paragraphs 107 and 108 of Akiyama as allegedly suggesting these recitations. Paragraphs 107 and 108 of Akiyama are presented above with respect to Claim 1.

As discussed above, in these areas, Akiyama merely discusses the use of only two keys, e.g. the master key Km and the channel key Kch, for encrypting and decrypting data in the broadcast station and the reception device. Encryption/decryption of data in Akiyama through the use of the master key Km and the channel key Kch operates differently from encoding/decoding data with the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) in the present invention. Akiyama nowhere suggests the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) that are recited in Claim 4. Furthermore, Akiyama provides no disclosure that would motivate one skilled in the art at the time the invention was made to arrive at the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) recited in Claim 4.

Applicant respectfully submits that these areas of Akiyama fail to anticipate, and Akiyama provides no motivation whatsoever to modify the teachings thereof to provide the recitations of Claim 4.

Additional features of the invention recited in Claim 4 are found in dependent Claim 5. Dependent Claim 5 recites, in part, that the data service providing apparatus of Claim 4 further includes a personal secret key storing unit for storing the personal secret key ({Ks}Kh) provided by the transmitting/receiving unit, and outputting the stored personal secret key ({Ks}Kh) to the first decoding unit under a control of the first decoding unit; and a cipher key storing unit for

storing the cipher key (Ks) obtained by the first decoding unit, and outputting the stored cipher key (Ks) to the second decoding unit under a control of the second decoding unit.

In the Final Office Action, the Examiner merely copied Claim 5 and identified FIGS. 3 and 14, and paragraphs 107 and 108 of Akiyama as allegedly suggesting these recitations. Paragraphs 107 and 108 of Akiyama are presented above with respect to Claim 1.

As discussed above, in these areas, Akiyama merely discusses the use of only two keys, e.g. the master key Km and the channel key Kch, for encrypting and decrypting data in the broadcast station and the reception device. Encryption/decryption of data in Akiyama through the use of the master key Km and the channel key Kch operates differently from encoding/decoding data with the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) in the present invention. Akiyama nowhere suggests the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) that are recited in Claim 5. Furthermore, Akiyama provides no disclosure that would motivate one skilled in the art at the time the invention was made to arrive at the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) recited in Claim 5.

Applicant respectfully submits that these areas of Akiyama fail to anticipate, and Akiyama provides no motivation whatsoever to modify the teachings thereof to provide the recitations of Claim 5.

Independent Claim 6 recites, in part, a security deciphering method comprising the steps of: determining whether or not a personal secret key ({Ks}Kh), generated by enciphering a cipher key (Ks) by using a hidden secret key (Kh) corresponding to intrinsic identification information, is received; if it is determined that the personal secret key ({Ks}Kh) is received, then decoding the received personal secret key ({Ks}Kh) by using the hidden secret key (Kh), thereby obtaining the cipher key (Ks); determining whether or not enciphered data ({M}Ks), generated by enciphering data (M) requested to be transmitted by using the cipher key (Ks), is received; and if

it is determined that the enciphered data ({M}Ks) is received, then decoding the enciphered data ({M}Ks) by using the cipher key Ks, thereby obtaining the data (M).

In the Final Office Action, the Examiner merely copied Claim 6 and identified paragraphs 108, 188, 195 and 198 of Akiyama as allegedly suggesting these recitations. Paragraph 108 is shown above with respect to Claim 1.

Paragraph 188 of Akiyama is shown below.

> "In the case where the appending information contains the channel sub-key H, a decryption unit 110 stores the channel sub-key H extracted from the appending information into a channel sub-key storage unit 508. Consequently, a channel decoder 509 can acquire the channel sub-key H from the channel sub-key storage unit 508 and combine it with the channel sub-key L delivered in a form of being multiplexed in the broadcast waves so as to generate the channel key Kch. Then, the contents information of the corresponding channel can be properly decrypted using the generated channel key Kch."

Paragraph 195 of Akiyama is shown below.

> "Each packet has a flag information that enables to distinguish whether that packet is a packet containing the master key seed, a packet containing the appending information, or a packet containing the contents information. In addition, the last packet for the master key seed and the appending information has an end flag recorded therein."

Paragraph 198 of Akiyama is shown below.

> "When it is Judged that the entered packet contains the appending information according to the flag of that packet, this packet is added to the buffer for the appending information, and when the end flag is detected in the flag of the sequentially entered packet, the packets stored in the buffer for the appending information up until then are transferred to a Judgement unit 507 (step S107 to S110)."

As discussed above, in these areas, Akiyama merely discusses the use of only two keys, e.g. the master key Km and the channel key Kch, for encrypting and decrypting data in the broadcast station and the reception device. Encryption/decryption of data in Akiyama through the use of the master key Km and the channel key Kch operates differently from encoding/decoding data with the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) in the present invention. Akiyama nowhere suggests the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) that are recited in each of the independent claims. Furthermore, Akiyama provides no disclosure that would motivate one skilled in the art at the time the invention was made to arrive at the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) recited in Claim 6.

Applicant respectfully submits that these areas of Akiyama fail to anticipate, and Akiyama provides no motivation whatsoever to modify the teachings thereof to provide the recitations of Claim 6.

Independent Claim 7 recites, in part, a data service providing method for providing data requested by a communication terminal, comprising the steps of: receiving via a public network a request for transmission of data (M) from the communication terminal; enciphering the data (M) by using a cipher key (Ks) in response to the received data transmission request, thereby generating enciphered data ({M}Ks); enciphering, in response to the received data transmission request, the cipher key (Ks) by using a hidden secret key (Kh) corresponding to intrinsic

identification information assigned to a security enciphering module equipped in the communication terminal to decode the enciphered data ({M}Ks), thereby generating personal secret key ({Ks}Kh); and transmitting the enciphered data ({M}Ks) and the personal secret key ({Ks}Kh) to the communication terminal via the public network.

In the Final Office Action, the Examiner merely copied Claim 7 and identified FIGS. 2 and 3, and paragraphs 107 and 108 of Akiyama as allegedly suggesting these recitations. Paragraphs 107 and 108 of Akiyama are presented above with respect to Claim 1.

As discussed above, in these areas, Akiyama merely discusses the use of only two keys, e.g. the master key Km and the channel key Kch, for encrypting and decrypting data in the broadcast station and the reception device. Encryption/decryption of data in Akiyama through the use of the master key Km and the channel key Kch operates differently from encoding/decoding data with the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) in the present invention. Akiyama nowhere suggests the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) that are recited in Claim 7. Furthermore, Akiyama provides no disclosure that would motivate one skilled in the art at the time the invention was made to arrive at the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) recited in Claim 7.

Applicant respectfully submits that these areas of Akiyama fail to anticipate, and Akiyama provides no motivation whatsoever to modify the teachings thereof to provide the recitations of Claim 7.

Additional features of the invention recited in Claim 7 are found in dependent Claim 8. Dependent Claim 8 recites, in part, that the security enciphering module equipped in the communication terminal comprises: a hidden secret key storing unit for storing the hidden secret key (Kh) corresponding to the intrinsic identification information assigned to the security enciphering module; a first decoding unit for decoding the personal secret key ({Ks}Kh) by using the hidden secret key (Kh), thereby obtaining the cipher key (Ks); and a second decoding unit for

decoding the enciphered data ({M}Ks) by using the obtained cipher key (Ks), thereby obtaining the data (M).

In the Final Office Action, the Examiner merely copied Claim 8 and identified FIGS. 2, 3 and 14, and paragraphs 107 and 108 of Akiyama as allegedly suggesting these recitations. Paragraphs 107 and 108 of Akiyama are presented above.

As discussed above, in these areas, Akiyama merely discusses the use of only two keys, e.g. the master key Km and the channel key Kch, for encrypting and decrypting data in the broadcast station and the reception device. Encryption/decryption of data in Akiyama through the use of the master key Km and the channel key Kch operates differently from encoding/decoding data with the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) in the present invention. Akiyama nowhere suggests the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) that are recited in Claim 8. Furthermore, Akiyama provides no disclosure that would motivate one skilled in the art at the time the invention was made to arrive at the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) recited in Claim 8.

Applicant respectfully submits that these areas of Akiyama fail to anticipate, and Akiyama provides no motivation whatsoever to modify the teachings thereof to provide the recitations of Claim 8.

Additional features of the invention recited in Claim 8 are found in dependent Claim 9. Dependent Claim 9 recites, in part, that the security deciphering module further comprises: a personal secret key storing unit for storing the personal secret key ({Ks}Kh) received by the communication terminal via the public network, and outputting the stored personal secret key ({Ks}Kh) to the first decoding unit under a control of the first decoding unit; and a cipher key storing unit for storing the cipher key (Ks) obtained by the first decoding unit, and outputting the stored cipher key (Ks) to the second decoding unit under a control of the second decoding unit.

In the Final Office Action, the Examiner merely copied Claim 9 and identified FIGS. 2, 3 and 14, and paragraphs 107 and 108 of Akiyama as allegedly suggesting these recitations. Paragraphs 107 and 108 of Akiyama are presented above with respect to Claim 1.

As discussed above, in these areas, Akiyama merely discusses the use of only two keys, e.g. the master key Km and the channel key Kch, for encrypting and decrypting data in the broadcast station and the reception device. Encryption/decryption of data in Akiyama through the use of the master key Km and the channel key Kch operates differently from encoding/decoding data with the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) in the present invention. Akiyama nowhere suggests the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) that are recited in Claim 9. Furthermore, Akiyama provides no disclosure that would motivate one skilled in the art at the time the invention was made to arrive at the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) recited in Claim 9.

Applicant respectfully submits that these areas of Akiyama fail to anticipate, and Akiyama provides no motivation whatsoever to modify the teachings thereof to provide the recitations of Claim 9.

Independent Claim 10 recites, in part, in a mobile communication terminal receiving, via a public network, enciphered data ({M}Ks) generated by enciphering data (M) by using a cipher key (Ks), a security deciphering apparatus comprising: a hidden secret key storing unit for storing a hidden secret key (Kh) corresponding to intrinsic identification information assigned to the mobile communication terminal; a first decoding unit for receiving a personal secret key ({Ks}Kh), generated by enciphering a cipher key (Ks) by using the hidden secret key (Kh), and decoding the personal secret key ({Ks}Kh) by using the hidden secret key (Kh), thereby obtaining the cipher key (Ks); and a second decoding unit for decoding the enciphered data ({M}Ks) by using the cipher key (Ks), thereby obtaining the data (M).

In the Final Office Action, the Examiner merely copied Claim 10 and identified FIG. 14, and paragraphs 107 and 108 of Akiyama as allegedly suggesting these recitations. Paragraphs 107 and 108 of Akiyama are presented above with respect to Claim 1.

As discussed above, in these areas, Akiyama merely discusses the use of only two keys, e.g. the master key Km and the channel key Kch, for encrypting and decrypting data in the broadcast station and the reception device. Encryption/decryption of data in Akiyama through the use of the master key Km and the channel key Kch operates differently from encoding/decoding data with the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) in the present invention. Akiyama nowhere suggests the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) that are recited in Claim 10. Furthermore, Akiyama provides no disclosure that would motivate one skilled in the art at the time the invention was made to arrive at the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) recited in Claim 10.

Independent Claim 11 recites, in part, a security deciphering method comprising: providing a hidden secret key (Kh) corresponding to intrinsic identification information; providing a cipher key (Ks); generating a personal secret key ({Ks}Kh) by the cipher key (Ks) by using the hidden secret key (Kh); and encoding/decoding data M using the hidden secret key (Kh), the cipher key (Ks); and the personal secret key ({Ks}Kh), thereby achieving improved security for transmitting/receiving the data M over public networks.

As discussed above, in these areas, Akiyama merely discusses the use of only two keys, e.g. the master key Km and the channel key Kch, for encrypting and decrypting data in the broadcast station and the reception device. Encryption/decryption of data in Akiyama through the use of the master key Km and the channel key Kch operates differently from encoding/decoding data with the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) in the present invention. Akiyama nowhere suggests the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) that are recited in Claim 11. Furthermore, Akiyama provides no disclosure that would motivate one skilled in the art to arrive

at the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) recited in Claim 11.

Applicant respectfully submits that these areas of Akiyama fail to anticipate, and Akiyama provides no motivation whatsoever to modify the teachings thereof to provide the recitations of Claim 11.

As described above, the present invention relates to a security deciphering apparatus and method in which the data of a cipher key used to encipher data is obtained by decoding an enciphered version of the cipher key by using hidden identification (ID) information given to a terminal requesting the data.

The present invention uses three keys including the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) to provide improvements in data security over prior art such as Akiyama because, as described above, the cipher key (Ks) used to encipher the data M requested by a communication terminal can only be obtained by decoding the personal secret key ({Ks}Kh) generated in accordance with an enciphering operation of the Ks enciphering unit, by using the hidden secret key (Kh) instrinsically assigned to the communication terminal.

The Examiner has erroneously stated, in the paragraph bridging the bottom of page 2 and the top of page 3 of the Final Office Action, that the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) are not recited in the claims. Despite this erroneous assertion by the Examiner, the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) are all recited in each of the independent claims.

Akiyama nowhere suggests the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) in accordance with the present invention. In addition, encryption/decryption of data in Akiyama through the use of the master key Km and the channel key Kch operates differently from encoding/decoding data with the hidden secret key (Kh), the cipher key (Ks), and the personal secret key ({Ks}Kh) in the present invention.

Applicant respectfully submits that Akiyama has failed to anticipate and provides no motivation whatsoever to modify the teachings thereof to provide a security deciphering apparatus comprising: a hidden secret key storing unit for storing a hidden secret key (Kh) corresponding to intrinsic identification information; a first decoding unit for receiving via a public network a personal secret key ({Ks}Kh), generated by enciphering a cipher key (Ks) by using the hidden secret key (Kh), and decoding the personal secret key ({Ks}Kh) by using the hidden secret key (Kh), thereby obtaining the cipher key (Ks); and a second decoding unit for receiving via the public network enciphered data ({M}Ks), generated by enciphering data (M) by using the cipher key (Ks), and decoding the enciphered data ({M}Ks) by using the cipher key (Ks), thereby obtaining the data (M), as recited in independent Claim 1 and similarly recited in independent Claims 3, 6, 7, 10, and 11.

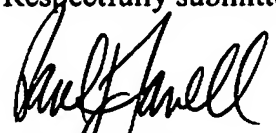
The Examiner has failed to establish a *prima facie* case of anticipation of Claims 1-10 based on Akiyama because there are differences between Akiyama and the recitations of Claims 1-10. It is well known that for a reference to anticipate a claim under 35 U.S.C. § 102(b) there "must be no difference between the claimed invention and the reference disclosure, as viewed by a person of ordinary skill in the field of the invention" (see *Scripps Clinic & Research Foundation v. Genentech Inc.*, 18 USPQ 2d 1001, 1010 (Fed. Cir. 1991). Furthermore, the Akiyama disclosure operates differently than the present invention and a "device which does not operate on the same principle cannot be an anticipation" (see *Los Alamitos Sugar Co. v. Carroll*, 173 F. 280, 284 (9th Cir. 1909).

Accordingly, Claims 1, 3, 6, 7, 10, and 11 are allowable over Akiyama.

While not conceding the patentability of the dependent claims, *per se*, Claims 2, 4, 5, 8 and 9 are also allowable for at least the above reasons.

Accordingly, all of the claims pending in the Application, namely, Claims 1-11, are in condition for allowance. Should the Examiner believe that a telephone conference or personal interview would facilitate resolution of any remaining matters, the Examiner may contact Applicant's attorney at the number given below.

Respectfully submitted,



Paul J. Farrell
Reg. No. 33,494
Attorney for Applicant

THE FARRELL LAW FIRM
333 Earle Ovington Blvd., Suite 701
Uniondale, New York 11553
Tel: (516) 228-3565
Fax: (516) 228-8475

PJF/TCS/dr